

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-251155
(43)Date of publication of application : 27.09.1996

(51)Int.Cl.

H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 07-048575
(22)Date of filing : 08.03.1995

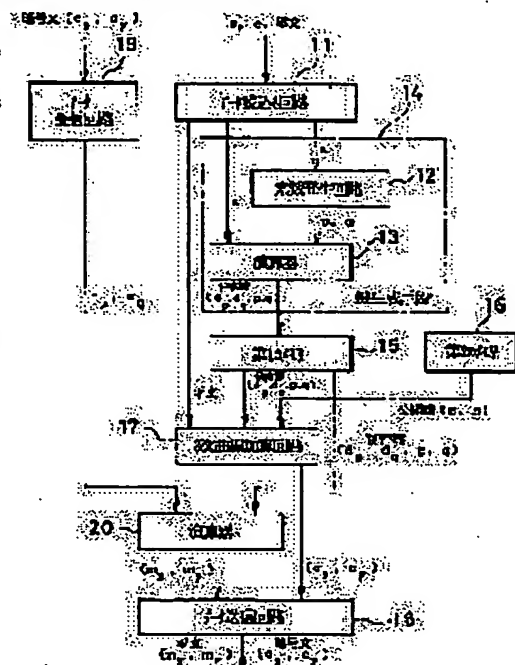
(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KOYAMA KENJI

(54) CIPHERING DEVICE, DECIPHERING DEVICE, CIPHERING AND DECIPHERING DEVICE AND CIPHER SYSTEM

(57)Abstract:

PURPOSE: To provide a ciphering device and a cipher system particularly excellent in the deciphering speed as compared with RSA ciphers in use.

CONSTITUTION: This device is provided with a key generation means 14 which generates primes p and q and at the time of computation with dp and dq satisfying $dp = (1/e) \bmod (p-1)$, $dq = (1/e) \bmod (q-1)$, where an integer e is mutually prime with the least common multiple of the product $n=pq$, $(p-1)$ and $(q-1)$, sets the product n and an integer e to be public keys and sets the primes p , q and dp , dq to be secret keys. In addition the device is provided with a ciphering calculation means which makes an integer pair of inputted plain texts correspond to a point on a cubic curve, determines a point obtained by e -folding the point by the use of the public keys by arithmetic on the cubic curve, and outputs arithmetic results as a cipher text, and a deciphering arithmetic means which subjects the integer pair of the inputted cipher text to homomorphic transformation, then raises the result to the dp -th power under a divisor p and dq -th power under a divisor q , and synthesizes them by the use of the Chinese remainder theorem to output a plain text.



LEGAL STATUS

[Date of request for examination] 08.03.1995
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2624634
[Date of registration] 11.04.1997
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Japanese Publication for Unexamined Patent Application

No. 8-251155/1996 (Tokukaihei 8-251155)

A. Relevance of the above-identified Document

This document has relevance to claims 1, 2, and 6 to 13 of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

(3)

($q-1$) の最小公倍数 N と、この最小公倍数 N と互いに素な整数 e に対し、

$$d_p = (1/e) \bmod (p-1), d_q = (1/e) \bmod (q-1)$$

を満たす d_p, d_q と計算したときの、積 n と整数 e とを公開鍵とすると共に、素数 p と q および前記 d_p と d_q とを秘密鍵とする鍵生成手段と、入力された暗号文の整数対を準同形変換した後に、法 p のもとで d_p 乗および q のもとで d_q 乗して、それらを中国剰余定理で合成して平文を出力する復号化暗号手段とを有する。

(0007) また、本発明 3 の発明は、素数 p と q とを生成して、これらの積 $n = pq$ と、($p-1$) および ($q-1$) の最小公倍数 N と、この最小公倍数 N と互いに素な整数 e に対し、

$$d_p = (1/e) \bmod (p-1), d_q = (1/e) \bmod (q-1)$$

を満たす d_p, d_q と計算したときの、積 n と整数 e とを公開鍵とすると共に、素数 p と q および前記 d_p と d_q とを秘密鍵とする鍵生成手段と、入力された平文の整数対を 3 次曲線上の点と対応させ、この点を前記公開鍵を用いて e 倍した点を前記 3 次曲線上の計算で求め、この計算結果を暗号文として出力する暗号化暗号手段と、入力された暗号文の整数対を準同形変換した後に、法 p のもとで d_p 乗および法 q のもとで d_q 乗して、それらを中国剰余定理で合成して平文を出力する復号化暗号手段とを有することを要旨とする。

(0008) さらに、本発明 4 の発明は、送信元から送られる平文の整数対を 3 次曲線上の点と対応させ、これを送信元の公開鍵との乗算を当該 3 次曲線上の計算で行なう暗号化手段と、この暗号化手段で暗号化された暗号文を前記送信元へ送り返す送信手段と、この送信手段を介して送られた暗号文を受信する受信手段と、この受信手段を介して受信した暗号文に対し、自己の秘密鍵による乗算を行なって復号化する復号化手段とを有することを要旨とする。

(0009)

[作用] 本発明によれば素数 p と q とを生成して、これらの積 $n = pq$ と、($p-1$) および ($q-1$) の最小公倍数 N と、その N と互いに素な整数 e に対し、

$$d_p = (1/e) \bmod (p-1), d_q = (1/e) \bmod (q-1)$$

を満たす d_p, d_q と鍵生成手段により計算されて、公開鍵 n と e と、秘密鍵 d_p, q および d_q とが作成られ、入力文の整数対が 3 次曲線上の点と対応させられ、その各整数対に対して、公開鍵 e により 3 次曲線上で乗算され、あるいは秘密鍵 d_p と d_q により整数上でべき乗算されて、暗号化され、または復号化される。

(0010)

[実施例] 以下、本発明に係る一実施例を図面を参照し

4

て説明する。図 1 は本発明に係る暗号・復号化装置の構成を示したブロック図である。

(0011) 図 1 に示すように、データ読み込み回路 11 は、鍵生成手段 14 および 3 次曲線加算回路 17 と接続される。この鍵生成手段 14 は、素数生成回路 12 と演算器 13 とで構成され、それぞれデータ読み込み回路 11 と接続され、共に素数生成回路 12 の出力は演算器 13 に接続される。また演算器 13 の出力は、第 1 のメモリ 15 に接続される。この第 1 のメモリ 15 の出力は 3 次曲線加算回路 17 と演算器 20 に接続される。第 2 のメモリ 16 の出力は 3 次曲線加算回路 17 に接続され、この 3 次曲線加算回路 17 の出力はデータ送回回路 18 に接続される。一方、データ受信回路 19 の出力は演算器 20 に接続され、さらにこの演算器 20 の出力はデータ送回回路 18 に接続される。

(0012) 次に、図 1 を参照して本実施例の作用を説明する。データ読み込み回路 11 に大きな適当な素数生成の種 s と、適当な小さい整数 e と、送信しようとする平文とが入力される。これらのうち種 s を用いて素数生成回路 12 で、素数 p と q とが生成される。

(0013) その素数 p, q と、データ読み込み回路 11 からの整数 e とが演算器 13 で供給され、 $n = pq$ の計算が行なわれる。通知は e の値として 3 または 5 を入力すればよい。この場合、これら整数 e と積 n は公開鍵とされ、 d_p, d_q は秘密鍵とされる。つまり素数生成回路 12 および演算器 13 は鍵生成手段 14 を構成している。秘密鍵 d_p, d_q, p, q は第 1 のメモリ 15 に記憶される。

(0014) データ読み込み回路 11 からの平文と、第 2 のメモリ 16 中の相手方、すなわち送信元の公開鍵 e, n とが 3 次曲線加算回路 17 で供給される。ここで平文の整数対 (m_x, m_y) を 3 次曲線上の点と対応させ、その整数対に相手方の公開鍵 e を 3 次曲線上の計算で乗算して暗号化する。つまり、特異な 3 次曲線 $y^2 + ax^3 = x^3$ の上の整数対 (x, y) を平文と対応させ

て計算する。

(0015) アフィン (affin) 座標では、3 次曲線上の 2 点、 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ が与えられたとき、これら 2 点の和 $P_3 = P_1 + P_2$ は次式で表される。

$$P_1 \neq P_2 \text{ のとき、}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = (y_2 - y_1) / (x_2 - x_1)$$

$$P_1 = P_2 \text{ のとき、}$$

$$x_3 = \lambda^2 - 2x_1$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

で計算される。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0022) まず、利用者 A の暗号化回路 21 の鍵生成手段 14 で生成された公開鍵 n_1, e_1 は送信回路 26 より送信回路 24 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 A の鍵として登録される。同時に利用者 B の暗号化回路 22 の鍵生成手段 14 で生成された公開鍵 n_2, e_2 は送信回路 26 より送信回路 25 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 B の鍵として登録される。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0023) 利用者 A が利用者 B へ通信文を暗号化して

(4)

$\lambda = (3x_1^2 - ay_1) / (2y_1 + ax_1)$

この加算公式は各点の座標系でも同様に適用できる。これらの加算公式を繰り返し適用して、ある点 P の整数倍の点 eP を求めることができる。つまり、 $5P$ は ($P + P + P + P + P$) と ($4P + P$) とにより求め、 $[0016]$ したがって、 $e(m_x, m_y)$ は、例えば上記の加算公式を繰り返すことにより求められる。また整数対 (m_x, m_y) が決まれば、これが位置する 3 次曲線 (a の値) は自動的に与えられ、加算公式を提供できる。また、この演算は ($\bmod n$) で行ない、つまり加算値が n を越え、その越えた方だけを加算結果とし

次に演算器 20 で整数対 d_p 乗および d_q 乗して、1 ※ [0018] 次元の平文 m_p と m_q を計算する。 ※ [数 2]

$$m_p = c_p \bmod p, m_q = c_q \bmod q$$

この m_p, m_q と a_p と a_q ★ [数 3]

$$c_p = \frac{c_1^3}{c_2^2} \bmod p, c_q = \frac{c_1^3}{c_2^2} \bmod q \quad \dots (1)$$

但し、 $s_p = \frac{c_1^3 - c_2^2}{c_1 c_2} \bmod p, s_q = \frac{c_1^3 - c_2^2}{c_1 c_2} \bmod q$ ★ [数 4]

から演算器 20 を用いて、それぞれ 3 次曲線上の整数対に換換する。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0022) まず、利用者 A の暗号化回路 21 の鍵生成手段 14 で生成された公開鍵 n_1, e_1 は送信回路 26 より送信回路 24 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 A の鍵として登録される。同時に利用者 B の暗号化回路 22 の鍵生成手段 14 で生成された公開鍵 n_2, e_2 は送信回路 26 より送信回路 25 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 B の鍵として登録される。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0023) 利用者 A が利用者 B へ通信文を暗号化して

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0022) まず、利用者 A の暗号化回路 21 の鍵生成手段 14 で生成された公開鍵 n_1, e_1 は送信回路 26 より送信回路 24 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 A の鍵として登録される。同時に利用者 B の暗号化回路 22 の鍵生成手段 14 で生成された公開鍵 n_2, e_2 は送信回路 26 より送信回路 25 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 B の鍵として登録される。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0023) 利用者 A が利用者 B へ通信文を暗号化して

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0022) まず、利用者 A の暗号化回路 21 の鍵生成手段 14 で生成された公開鍵 n_1, e_1 は送信回路 26 より送信回路 24 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 A の鍵として登録される。同時に利用者 B の暗号化回路 22 の鍵生成手段 14 で生成された公開鍵 n_2, e_2 は送信回路 26 より送信回路 25 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 B の鍵として登録される。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0023) 利用者 A が利用者 B へ通信文を暗号化して

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0022) まず、利用者 A の暗号化回路 21 の鍵生成手段 14 で生成された公開鍵 n_1, e_1 は送信回路 26 より送信回路 24 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 A の鍵として登録される。同時に利用者 B の暗号化回路 22 の鍵生成手段 14 で生成された公開鍵 n_2, e_2 は送信回路 26 より送信回路 25 を通じてセンタ装置 23 内の暗号ファイル 27 に利用者 B の鍵として登録される。

また、暗号化回路 21、22 のそれぞれの構成は、図 1 に示した暗号化回路とは同一であり、対応する部分には同一符号を付してある。

(0023) 利用者 A が利用者 B へ通信文を暗号化して

(5)

7 送信する場合は、利用者Aは通信線24を通じてセンタ装置23から、利用者Bの公開鍵 n_2, e_2 を受け取り、前述した第1の実施例で示されるアルゴリズムに従って暗号化し、その暗号文の整数対を送信回路18を通じて通信線28へ送出する。

10 0 2 4 利用者Bの暗号装置22では、通信線28から受信回路19に受信された暗号文は、前記の通り復号化されて、元の平文が復元される。利用者Bから利用者Aへの暗号通信も同様に行なわれ、この場合は鍵 n_1, e_1, d_1, p, q が用いられる。

10 0 2 5 以上説明したように本実施例は、次の長所をもっている。

(1) 本実施例の暗号方式は従来のRSA暗号に比べて、復号化速度が約2倍であり、暗号化速度はほぼ同じである。RSA暗号は通常、復号に時間がかかっていたので、本実施例の方式では全体の速度向上が約2倍となっている。

(2) 本実施例の暗号方式はRSA暗号と同じレベルの安全性をもつ。

10 0 2 6 〔発明の効果〕 以上説明したように本発明は、従来のRSA暗号に比べて、復号化速度が約2倍と高速でありながら、暗号化速度及び安全性はほぼ同じであるとい

8

う優れた効果を備える。

〔図面の簡単な説明〕

〔図1〕 本発明に係る暗号装置の一実施例の概略の構成を示すブロック図である。

〔図2〕 本発明に係る暗号システムの一実施例を示すブロック図である。

11 データ読み込み回路

12 素数生成回路

13 演算器

14 鍵生成手段

15 第1のメモリ

16 第2のメモリ

17 3次曲線加算回路

18 データ送信回路

19 データ受信回路

20 演算器

21 暗号装置

22 暗号装置

23 センタ装置

24, 25, 28 通信線

26 送受信器

27 鍵ファイル

(6)

〔図1〕

